FORTINET®

FortiOS - Release Notes

Version 6.4.12

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 27, 2023
FortiOS 6.4.12 Release Notes
01-6412-880653-20230227

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-02-23	Initial release.
2023-02-27	Updated Known issues on page 31.

Introduction and supported models

This guide provides release information for FortiOS 6.4.12 build 2060.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.12 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-400E-BP, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
FortiFirewall	FFW-3980E, FFW-4200F, FFW-4400F, FFW-VM64, FFW-VM64-KVM
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 6.4.12. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 2060.

FFW-1801F	is released on build 5424.
FFW-2600F	is released on build 5424.
FFW-4401F	is released on build 5424.

Special notices

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

System Advanced menu removal (combined with System Settings)

Bug ID	Description
584254	• Removed *System* > *Advanced* menu (moved most features to *System* > *Settings* page). • Moved configuration script upload feature to top menu > *Configuration* > *Scripts* page. • Removed GUI support for auto-script configuration (the feature is still supported in the CLI). • Converted all compliance tests to security rating tests.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

FG-80E-POE and FG-81E-POE PoE controller firmware update

FortiOS 6.4.0 has resolved bug 570575 to fix a FortiGate failing to provide power to ports. The PoE hardware controller, however, may require an update that must be performed using the CLI. Upon successful execution of this command, the PoE hardware controller firmware is updated to the latest version 2.18:

```
diagnose poe upgrade-firmware
```

AWS-On-Demand image

Bug ID	Description
589605	Starting from FortiOS 6.4.0, the FG-VM64-AWSONDEMAND image is no longer provided. Both AWS PAYG and AWS BYOL models will share the same FG-VM64-AWS image for upgrading and new deployments. Remember to back up your configuration before upgrading.

Azure-On-Demand image

Bug ID	Description
657690	Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

FortiClient EMS Cloud registration

FortiOS 6.4.3 adds full support for FortiClient EMS Cloud service. Users will be able to register and use the service in mid-December 2020.

SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 and 6.4.3 ended support for TLS 1.0 when `strong-crypto` is enabled under `system global`. With this change, SSL traffic over TLS 1.0 will not be checked so it will be bypassed by default.

To examine and/or block TLS 1.0 traffic, an administrator can either:

- Disable `strong-crypto` under `config system global`. This applies to FortiOS 6.2.6 and 6.4.3, or later versions.
- Under `config firewall ssl-ssh-profile`:
  - in FortiOS 6.2.6 and later, set `unsupported-ssl` to `block`.
  - in FortiOS 6.4.3 and later, set `unsupported-ssl-negotiation` to `block`.

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 6.4.7.

Hyperscale firewall support

FortiOS 6.4.12 supports hyperscale firewall features for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F). For more information, refer to the Hyperscale Firewall Release Notes.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
776052	Add four SNMP OIDs for polling critical port block allocations (PBAs) IP pool statistics including: • Total PBAs: fgFwIppStatsTotalPBAs (1.3.6.1.4.1.12356.101.5.3.2.1.1.9) • In use PBAs: fgFwIppStatsInusePBAs (1.3.6.1.4.1.12356.101.5.3.2.1.1.10) • Expiring PBAs: fgFwIppStatsExpiringPBAs (1.3.6.1.4.1.12356.101.5.3.2.1.1.11) • Free PBAs: fgFwIppStatsFreePBAs (1.3.6.1.4.1.12356.101.5.3.2.1.1.12)

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Device detection changes

In FortiOS 6.0.x, the device detection feature contains multiple sub-components, which are independent:

- Visibility – Detected information is available for topology visibility and logging.
- FortiClient endpoint compliance – Information learned from FortiClient can be used to enforce compliance of those endpoints.
- Mac-address-based device policies – Detected devices can be defined as custom devices, and then used in device-based policies.

In 6.2, these functionalities have changed:

- Visibility – Configuration of the feature remains the same as FortiOS 6.0, including FortiClient information.
- FortiClient endpoint compliance – A new fabric connector replaces this, and aligns it with all other endpoint connectors for dynamic policies. For more information, see Dynamic Policy - FortiClient EMS (Connector) in the *FortiOS 6.2.0 New Features Guide*.
- MAC-address-based policies – A new address type is introduced (MAC address range), which can be used in regular policies. The previous device policy feature can be achieved by manually defining MAC addresses, and then adding them to regular policy table in 6.2. For more information, see MAC Addressed-Based Policies in the *FortiOS 6.2.0 New Features Guide*.

If you were using device policies in 6.0.x, you will need to migrate these policies to the regular policy table manually after upgrade. After upgrading to 6.2.0:

1. Create MAC-based firewall addresses for each device.
2. Apply the addresses to regular IPv4 policy table.

In 6.4.0, device detection related GUI functionality has been relocated:

1. The device section has moved from *User & Authentication* (formerly *User & Device*) to a widget in *Dashboard*.
2. The email collection monitor page has moved from *Monitor* to a widget in *Dashboard*.

In 6.4.4, a new sub-option, *Delete*, was added when right-clicking on the device. This option is not available when the device is online, or the device is retrieved from FortiClient.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.4.12 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.4.10
- FortiManager 6.4.10
- FortiClient EMS 6.4.3 build 1600 or later
- FortiClient 6.4.3 build 1608 or later
- FortiAP 6.4.4 build 0456 or later
- FortiSwitch 6.4.5 build 0461 or later

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC

13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice

⚠ If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.12. When Security Fabric is enabled in FortiOS 6.4.12, all FortiGate devices must be running FortiOS 6.4.12.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.12 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.4.12 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.4.12 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.4.12 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5	Inf1	P3	T3a
C5d	m4.16xlarge	R4	u-6tb1.metal
C5n	M5	R5	u-9tb1.metal
F1	M5a	R5a	u-12tb1.metal
G3	M5ad	R5ad	u-18tb1.metal
G4	M5d	R5d	u-24tb1.metal
H1	M5dn	R5dn	X1
I3	M5n	R5n	X1e
I3en	P2	T3	z1d

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.4.12, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.4.12.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix Hypervisor 8.1 Express Edition

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V Server 2019 and Windows Server 2012R2 with Hyper-V role

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

Monitor widgets can be saved as standalone dashboards.

There are two types of default dashboard settings:

- Optimal: Default dashboard settings in 6.4.1
- Comprehensive: Default Monitor and FortiView settings before 6.4.1

Filtering facets are available for FortiView widgets in full screen and standalone mode.

WanOpt configuration changes in 6.4.0

Port configuration is now done in the profile protocol options. HTTPS configurations need to have certificate inspection configured in the firewall policy.

In FortiOS 6.4.0, `set ssl-ssh-profile certificate-inspection` must be added in the firewall policy:

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
    next
end
```

WanOpt and web cache statistics

The statistics for WanOpt and web cache have moved from *Monitor* to a widget in *Dashboard*.

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.2.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Virtual WAN link member lost

The member of `virtual-wan-link` is lost after upgrade if the `mgmt` interface is set to `dedicated-to management` and part of an SD-WAN configuration before upgrade.

Enabling match-vip in firewall policies

As of FortiOS 6.4.3, `match-vip` is not allowed in firewall policies when the action is set to accept.

Hardware switch members configurable under system interface list

Starting in FortiOS 6.4.7, hardware switch members are also shown under `config system interface` with limited configuration options available.

VDOM link and policy configuration is lost after upgrading to 6.4.9 and later or 7.0.6 and later

There is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step. A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

Product integration and support

The following table lists FortiOS 6.4.12 product integration and support information:

Web Browsers	• Microsoft Edge • Mozilla Firefox version 103 • Google Chrome version 104 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 14. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 14. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.4.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 14 and Fortinet Security Fabric upgrade on page 14. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.
FortiClient iOS	• 6.4.0 and later
FortiClient Android and FortiClient VPN Android	• 6.4.0 and later
FortiClient EMS	• 6.4.0
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0309 and later (needed for FSSO agent support OU in group filters) • Windows Server 2022 Standard • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 4.2 version.
AV Engine	• 6.00172
IPS Engine	• 6.00155
Virtualization Environments	
Citrix	• Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	• Windows Server 2012R2 with Hyper-V role • Windows Hyper-V Server 2019
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 103 Google Chrome version 104
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 103 Google Chrome version 104
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 103 Google Chrome version 104
macOS Big Sur 11.0	Apple Safari version 15 Mozilla Firefox version 103 Google Chrome version 104
iOS	Apple Safari

Operating System	Web Browser
	Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 6.4.12. To inquire about a particular bug, please contact Customer Service & Support.

Explicit Proxy

Bug ID	Description
763796	FTP proxy refuses a connection on a freshly configured FortiGate.
774442	WAD is NATting to the wrong IP pool address for the interface.

GUI

Bug ID	Description
794757	Inbound traffic on the interface bandwidth widget shows *0 bps* on the VLAN interface.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
750978	Interface link status of HA members go down when `cfg-revert` tries to reboot post `cfg-revert-timeout`.
785514	In some cases, the fgfmd daemon is blocked by a query to the HA secondary checksum, and it will cause the tunnel between FortiManager and the FortiGate to go down.
838541	HA is out-of-sync due to `certificate local` in FGSP standalone cluster.

Hyperscale

Bug ID	Description
805846	In the FortiOS MIB files, the trap fields `fgFwIppStatsGroupName` and `fgFwIppStatsInusePBAs` have the same OID. As a result, the `fgFwIppStatsInusePBAs` field always returns a value of `0`.

IPsec VPN

Bug ID	Description
675838	iked ignores phase 1 configuration changes due to frequent FortiExtender CMDB changes.
855772	FortiGate IPsec tunnel role could be incorrect after rebooting or upgrading, and causes negotiation to be stuck when it comes up.
858715	IPsec phase 2 fails when both HA cluster members reboot at the same time.

Log & Report

Bug ID	Description
838357	A deny policy with log traffic disabled is generating logs.

Proxy

Bug ID	Description
650348	FortiGate refuses incoming TCP connection to FTP proxy port after explicit proxy related configurations are changed.
799381	WAD crash occurs when TLS 1.2 receives the client certificate and that server-facing SSL port has been closed due to the SSL bypass.

Routing

Bug ID	Description
817670	IPv6 route redistribution metric value is not taking effect.

Security Fabric

Bug ID	Description
837347	Upgrading from 6.4.8 to 7.0.5 causes SDN firewall address configurations to be lost.
843043	Only the first ACI SDN connector can be kept after upgrading from 6.4.8 if multiple ACI SDN connectors are configured.
857441	Azure Fabric connector process (azd) has high memory consumption during updates, which leads to low-end FortiGate models entering conserve mode.

SSL VPN

Bug ID	Description
705880	Updated empty group with SAML user does not trigger an SSL VPN firewall policy refresh, which causes the SAML user detection to not be successful in later usage.
742332	SSL VPN web portal redirect fails in http://qu***.jj***.bu***.
746230	SSL VPN web mode cannot display certain websites that are internal bookmarks.
748085	Authentication request of SSL VPN realm can now only be sent to user group, local user, and remote group that is mapped to that realm in the SSL VPN settings. The authentication request will not be applied to the user group and remote group of non-realm or other realms.
784522	When trying to create a support ticket in Jira with SSL VPN proxy web mode, the dropdown field does not contain any values.
822432	SSL VPN crashes after copying a string to the remote server using the clipboard in RDP web mode when using RDP security.
825810	SSL VPN web mode is unable to access EMS server.
834713	Getting re-authentication pop-up window for VNC quick connection over SSL VPN web proxy.
848067	RDP over VPN SSL web mode stops work after upgrading to 6.4.10.
852566	User peer feature for one group to match to multiple user peers in the authentication rules is broken.
854143	Unable to access Synology NAS server through SSL VPN web mode.

Bug ID	Description
856316	Browser displays an *Error, Feature is not available* message if a file larger than 1 MB is uploaded from FTP or SMB using a web bookmark, even though the file is uploaded successfully. There are no issues with downloading files.

Switch Controller

Bug ID	Description
845667	Enabling `allowed-vlans-all` on FortiSwitch ports will push VLANs from both owner and tenant VDOMs.
859690	The flcfgd daemon crashes frequently on the HA passive unit.

System

Bug ID	Description
649729	HA synchronization packets are hashed to a single queue when `sync-packet-balance` is enabled.
713951	Not all ports are coming up after an LAG bounce on 8 × 10 GB LAG with ASR9K. Affected platforms: FG-3960E and FG-3980E.
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected.
733096	FG-100F HA secondary's unused ports flaps from down to up, then to down.
776052	Add SNMP MIB support for PBA pools.
783939	IPv4 session is flushed after creating a new VDOM.
784169	When a virtual switch member port is set to be an alternate by STP, it should not reply with ARP; otherwise, the connected device will learn the MAC address from the alternate port and send subsequent packets to the alternate port.
787929	Deleting a VDOM that contains EMAC interfaces might affect the interface bandwidth widget of the parent VLAN.
807334	DDNS is not working when cleartext is enabled.
810466	EHP and HRX drop on NP6 FortiGate, causing low throughput.
811367	Ports 33-35 constantly show suspect messaging in the transceiver output. Affected platforms: FG-2600F and FG-2601F.

Bug ID	Description
813607	LACP interfaces are flapping after upgrading to 6.4.9.
815692	Slow upload speeds when connected to FIOS connection. Affected platforms: NP6Lite and NP6xLite.
821000	QSFP and QSFP+ Fortinet transceivers are not operational on FG-3401E.
824543	The `reply-to` option in the email server settings is no longer visible in a default server configuration.
827240	FortiGate in HA may freeze and reboot. Before the reboot, softIRQ may be seen as high. This leads to a kernel panic.
827736	As the size of the internet service database expands, `ffdb_err_msg_print: ret=-4, Error: kernel error` is observed frequently on 32-bit CPU platforms, such as the FG-100E.
834850	GUI CLI console displays a `Connection lost` message when logging in as an API administrator.
847077	`Can't find xitem. Drop the response.` error appears for DHCPOFFER packets in the DHCP relay debug.
850774	Session synchronization packets may be dropped when using HA1/HA2. Affected platforms: FGT-420xF and FGT-440xF.

Upgrade

Bug ID	Description
848926	After upgrading, the AV filter feature set is changed from proxy mode to flow mode.

User & Authentication

Bug ID	Description
751763	When MAC-based authentication is enabled, multiple RADIUS authentication requests may be sent at the same time. This results in duplicate sessions for the same device.
824999	Subject Alternative Name (SAN) is missing from the certificate upon automatic certificate renewal made by the FortiGate.
845198	Local-in policies for authentication disappear and the authentication page returns a *ERR_CONNECTION_TIMED_OUT* error. The authentication page is not displayed because it is not rebuilt when `firewall local-in-policy` is added, edited, or deleted.
853793	FG-81F 802.1X MAC authentication bypass (MAB) failed to authenticate Cisco AP.

WiFi Controller

Bug ID	Description
761836	FWF-8xF platforms should allow the DHCP server configuration of an aggregate interface (aplink) to be edited in the GUI.
807713	FortiGate is not sending RADIUS accounting message consistently to RADIUS server for wireless SSO.

Known issues

The following issues have been identified in version 6.4.12. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
752420	If a .TAR.BZ2 or .TAR.GZ archive contains an archive bomb inside its compressed stream, the AV engine will time out.

Firewall

Bug ID	Description
727809	Disabled deny firewall policy with virtual server objects cannot be enabled after a firewall reboot.
739949	In HA virtual cluster scenario, the *Bytes* counter on the *Firewall Policy* page always shows *0 B* for the secondary while the *Edit Policy* page shows the correct *Total bytes* in the statistics.

FortiView

Bug ID	Description
683654	FortiView pages with FortiAnalyzer source incorrectly display a *Failed to retrieve data* error on all VDOM views when there is a newly created VDOM that is not yet registered to FortiAnalyzer. The error should only show on the new VDOM view.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches.
653952	*The web page cannot be found* is displayed when a dashboard ID no longer exists. **Workaround**: load another page in the navigation pane. Once loaded, load the original dashboard page (that displayed the error) again.
688016	GUI interface bandwidth widget does not show correct data for tunnel interface when ASIC offload is enabled on the firewall policy.
695163	When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI *Forward Traffic* log page can take time to load if there is no specific filter for the time range. **Workaround**: provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs.
722358	When a FortiGate local administrator is assigned to more than two VDOMs and tries logging in to the GUI console, they get a command parse error when entering VDOM configuration mode.
743477	On the *Log & Report* > *Forward Traffic* page, filtering by the *Source* or *Destination* column with negation on the IP range does not work.
748530	A gateway of *0.0.0.0* is not accepted in a policy route.
829665	User randomly lost GUI access, and the httpsd process is in a D state.
843554	The ALL service object is changed when a new object is created.

HA

Bug ID	Description
771999	Sessions not synchronized to HA secondary on an FGSP and FGCP combined setup.
776355	Packet loss occurs on the software switch interface when a passive device goes down.
779180	FGSP does not synchronize the `helper-pmap` expectation session.
816883	High CPU usage on secondary device, and CPU lacks the AVX feature needed to load `libdpdk.so`.
830879	Running `execute ha manage 0 <remote_admin>` fails and displays a `Permission denied, please try again.` error if the 169.254.0.0/16 local subnet is not in the trusted host list.

Bug ID	Description
832634	HA failovers occur due to the kernel hanging on FG-100F.
856643	FG-500E interface stops sending IPv6 RAs after upgrading.

Hyperscale

Bug ID	Description
734305	In the GUI, an FQDN or ISDB can be selected for a DoS policy, which is not supported (an error message appears). The CLI shows the correct options.
760560	The timestamp on the hyperscale SPU of a deny policy (policy id 0) is incorrect.
796368	Traffic shaping profile does not seem to have an effect on TCP/UDP traffic in hyperscale.
802369	Large client IP range makes fixed allocation usage relatively limited.

Intrusion Prevention

Bug ID	Description
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.
763736	IPS custom signature logging shows (even after being disabled) after upgrading to FortiOS 6.4.7.
873975	Source MAC changes and the packet drops due to both sides of the session using the same source MAC address.

IPsec VPN

Bug ID	Description
787590	ADVPN is not negotiated after gateway re-validation.
805301	Enabling NPU offloading in the phase 1 settings causes a complete traffic outage after a couple of ping packets pass through.
840153	Unexpected dynamic selectors block traffic when `set mesh-selector-type subnet` is configured.

Proxy

Bug ID	Description
604681	WAD process with SoC SSL acceleration enabled consumes more memory usage over time, which may lead to conserve mode. **Workaround**: disable SoC SSL acceleration under the firewall SSL settings.

REST API

Bug ID	Description
759675	`Connection failed` error occurs on FortiGate when an interface is created and updated using the API in quick succession.

Routing

Bug ID	Description
618684	When HA failover is performed to the other cluster member that is not able to reach the BFD neighbor, the BFD session is down as expected but the static route is present in the routing table.
797590	GRE tunnel configured using a loopback interface is not working after changing the interface back and forth.
860075	Traffic session is processed by a different SD-WAN rule and randomly times out.
862418	Application VWL crash occurs after FortiManager configuration push causes an SD-WAN related outage.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.

SSL VPN

Bug ID	Description
730416	Forward traffic log does not generate logs for HTTP and HTTPS services with SSL VPN web mode.
781581	Customer internal website is not shown correctly in SSL VPN web mode.
803622	High CPU in SSL VPN once SAML is used with FortiAuthenticator and an LDAP server.
818196	SSL VPN does not work properly after reconnecting without authentication and a TX drop is found.
850898	OS checklist for the SSL VPN in FortiOS does not include macOS Ventura (13).

Switch Controller

Bug ID	Description
798724	FortiSwitch exported ports in tenant VDOM are gone after rebooting the FortiGate.

System

Bug ID	Description
555616	When NTurbo is enabled, it is unexpectedly provided with the wrong traffic direction information (from server or from client) to decide the destination for the data. This causes the traffic to be sent back to the port where it came from.
602141	The extender daemon crashes on Low Encryption (LENC) FortiGates.
648085	Link status on peer device is not down when the admin port is down on the FortiGate.
664856	A VWP named .. can be created in the GUI, but it cannot be edited or deleted.
669645	VXLAN VNI interface cannot be used with a hardware switch.
685674	FortiGate did not restart after restoring the backup configuration via FortiManager after the following process: disable NPU offloading, change NGFW mode from profile-based to policy-based, retrieve configuration from FortiGate via FortiManager, and install the policy package via FortiManager.
688009	Update built-in modem firmware that comes with the device in order for the SIM to be correctly identified and make LTE link work properly.
705878	Local certificates could not be saved properly, which caused issues such as not being able to properly restore them with configuration files and causing certificates and keys to be mismatched.
709679	Get `can not set mac address(16)` error message when setting a MAC address on an interface in HA that is already set.

Bug ID	Description
729912	DNS proxy does not transfer the DNS query for IPv6 neighbor discovery (ND) when client devices are using random MAC addresses, so one device can configure many IPv6 addresses.
751715	Random LTE modem disconnections due to certain carriers getting unstable due to WWAN modem USB speed under super-speed.
753421	Slow SNMP query performance of fgVpn2Tables OIDs when a large number of IPsec dialup tunnels are connected.
766834	forticron allocates over 700 MB of memory, causes the FortiGate to go into conserve mode, and causes kernel panic due to 100 MB of configured CRL.
782962	PSU alarm log and SNMP trap are added for FG-10xF and FG-8xF models.
796094	Egress traffic on EMAC VLAN is using base MAC address instead.
800295	NTP server has intermittent unresolvable logs after upgrading to 6.4.
818795	Kernel panic observed on FG-3700D.
844937	FG-3700D unexpectedly reboots after the COMLog reported a kernel panic due to an IPv6 failure to set up the master session for the expectation session under some conditions.
850430	DHCP relay does not work properly with two DHCP relay servers configured.
850683	Console keeps displaying `bcm_nl.nr_request_drop ...` after the FortiGate reboots because of the `cfg-save revert` setting under `config system global`. Affected platforms: FG-10xF and FG-20xF.
850688	FG-20xF system halts if setting `cfg-save` to `revert` under `config system global` and after the `cfg-revert-timeout` occurs.
855151	There may be a race condition between the CMDB initializing and the customer language file loading, which causes the customer language file to be removed after upgrading. **Workaround**: re-upload the customer language file after the FortiGate boots up.

Upgrade

Bug ID	Description
743389	The `dnsfilter-profile` setting was purged from all DNS server entries upon upgrading from before 6.4.4.
767808	The `asicdos` option for enabling/disabling NP6XLite DoS offloading is missing after upgrading to 6.4.9. Affected platforms: NP6XLite.
840921	When upgrading from 6.0.15 to 6.4.11, an existing explicit flow-based web filter profile changes to proxy-based.

User & Authentication

Bug ID	Description
778521	SCEP fails to renew if the local certificate name length is between 31 and 35 characters.

VM

Bug ID	Description
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
617046	FG-VMX manager not showing all the nodes deployed.
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
764392	Incorrect VMDK file size in the OVF file for hw13 and hw15. **Workaround**: manually correct the hw13 and hw15 OVF file's `ovf:size` value.

Web Filter

Bug ID	Description
779278	FortiGate is responding on TLS 1.0, TLS 1.1, and SSLv3 on TCP port 8015.
789804	Web filter configured to restrict YouTube access does not work.

WiFi Controller

Bug ID	Description
662714	The `security-redirect-url` setting is missing when the `portal-type` is `auth-mac`.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
773711	HTTPS sessions to some internal destinations are randomly dropped for users from the same group set.
822551	EICAR virus test file HTTPS traffic cannot be blocked, even when there is a block IPS log.
836955	Primary and secondary units of HA cluster are not accessible and drop traffic.
838875	Application control `filename` field has unexpected character and breaks the syslog format.
839671	IPS engine is crashing.
847129	IPS engine crashes and FortiGate enters conserve mode. IPS engine stalled and IPS fail-open is triggered.
848368	IPS is causing high memory (FortiOS 6.4.8)
855301	IPS engine is consuming high memory.
856616	High IPS engine memory usage after device upgrade.
856793	After changing the static URL file, network degradation occurs and impacts the end-user traffic.
863074	Both `block` and `passthrough` logs are sent out by the web filter override function.
870243	ZIP file block does not work as expected with flow-mode DLP.
873153	URLs longer than 8000 characters are unable to get a FortiGuard rating with flow-based URL filter.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.